

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-143359

(43)Date of publication of application : 28.05.1999

(51)Int.Cl.

G09C 1/00  
H04L 9/08

(21)Application number : 09-308679

(71)Applicant : MITSUBISHI MATERIALS CORP

(22)Date of filing : 11.11.1997

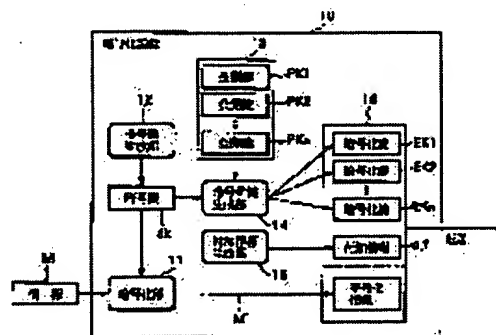
(72)Inventor : OOKUBO TATSUMASA  
TOYODA SHOICHI

(54) ENCIPHERING DEVICE, DECODING DEVICE, INFORMATION SHARING DEVICE, ENCIPHERING METHOD, DECODING METHOD, INFORMATION PROCESSING METHOD, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable sharing secret information by plural users by coding a code key used for enciphering with an open key of at least one user with which information can be seen, and generating plural enciphering keys.

SOLUTION: An enciphering section 11 codes input information M using an enciphering key dk for enciphering information, for example, by a sharing key cipher system, generates enciphering information M', and outputs it to a transfer section 16. A cipher key generating section 12 is constituted with random numbers generating circuit and the like, generates a coding key dk for enciphering information, and outputs it to the coding section 11 and an enciphering key generating section 14. And, the coding key generating section 14 enciphers information M using an open key of a user recorded in a storage section 13 based on an open key cipher system, generates plural enciphering keys EK1, EK2,...EKn, and outputs generated plural enciphering keys EK1-EKn to the transfer section 16.



## LEGAL STATUS

[Date of request for examination] 31.03.2000

[Date of sending the examiner's decision of rejection] 30.03.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-143359

(43) 公開日 平成11年(1999) 5月28日

(51) Int.Cl.<sup>6</sup>  
G 0 9 C 1/00  
H 0 4 L 9/08

識別記号  
6 3 0

F I  
G 0 9 C 1/00 6 3 0 D  
6 3 0 E  
H 0 4 L 9/00 6 0 1 E  
6 0 1 D

審査請求 未請求 請求項の数51 O L (全 16 頁)

(21) 出願番号 特願平9-308679

(22) 出願日 平成9年(1997)11月11日

(71) 出願人 000006264

三菱マテリアル株式会社  
東京都千代田区大手町1丁目5番1号

(72) 発明者 大久保 達真

埼玉県大宮市北袋町1丁目297番地 三菱  
マテリアル株式会社総合研究所内

(72) 発明者 豊田 祥一

埼玉県大宮市北袋町1丁目297番地 三菱  
マテリアル株式会社総合研究所内

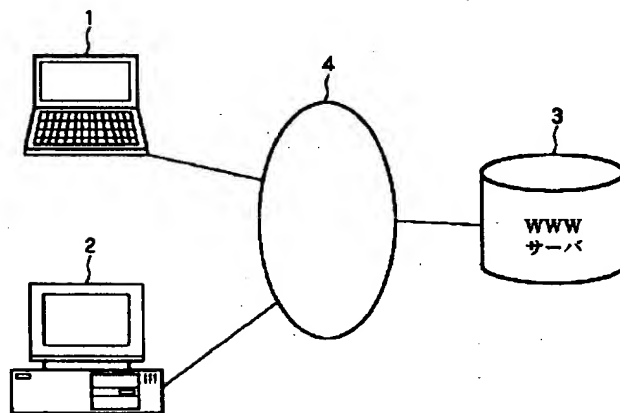
(74) 代理人 弁理士 佐藤 隆久

(54) 【発明の名称】 暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体

(57) 【要約】

【課題】 秘匿情報の複数ユーザによる共有が可能で、情報の内容の漏洩を防止できる暗号化装置、復号化装置を備えた情報共有システム等を提供する。

【解決手段】 サーバ3と、暗号化情報を生成する暗号化部11と、暗号鍵をユーザの公開鍵で暗号化し複数の暗号化鍵を生成する暗号化鍵生成部14と、複数の暗号化鍵がどのユーザの公開鍵で暗号化されたものかを特定する付加情報を生成する付加情報生成部15と、複数の暗号化鍵、暗号化情報および付加情報をサーバ3に保管させる転送部16とを有する暗号化装置10と、保管された複数の暗号化鍵を取得してユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号化鍵復号化部21と、付加情報を取得して複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択部22と、この暗号鍵に基づき暗号化情報を復号して元の情報を取得する情報復号化部23とを有する復号化装置20とを設ける。



## 【特許請求の範囲】

【請求項 1】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、

暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段とを有する暗号化装置。

【請求項 2】 上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段とを有する暗号化装置。

【請求項 3】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 2 記載の暗号化装置。

【請求項 4】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 2 記載の暗号化装置。

【請求項 5】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 2、3 または 4 記載の暗号化装置。

【請求項 6】 上記複数の暗号化鍵および暗号化情報を転送する転送手段とを有する請求項 1 記載の暗号化装置。

【請求項 7】 上記複数の暗号化鍵、暗号化情報、および付加情報を転送する転送手段とを有する請求項 2、3、4 または 5 記載の暗号化装置。

【請求項 8】 上記転送手段は、情報を複数のユーザでアクセス可能な情報保管手段に転送する請求項 6 または 7 記載の暗号化装置。

【請求項 9】 複数の暗号化鍵および暗号化情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項 10】 複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する暗号鍵取得手段と、上記付加情報に基づいて上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項 11】 複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化

されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、

上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、

上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項 12】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 10 または 11 記載の復号化装置。

【請求項 13】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 10 または 11 記載の復号化装置。

【請求項 14】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 10、11、12 または 13 記載の復号化装置。

【請求項 15】 取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段とを有する請求項 14 記載の復号化装置。

【請求項 16】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、

上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項 17】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、およ

び付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、

上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号化鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号化鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項 1 8】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、

上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号化鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項 1 9】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 1 7 または 1 8 記載の情報共有システム。

【請求項 2 0】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 1 7 または 1 8 記載の情報共有システム。

【請求項 2 1】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 1 7、1 8、1 9 または 2 0 記載の情報共有システム。

【請求項 2 2】 取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段を有する請求項 2 1 記載の情報共有システム。

ム。

【請求項 2 3】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号化鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第 1 の装置と、

上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第 2 の装置とを有する情報共有システム。

【請求項 2 4】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号化鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第 1 の装置と、

上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第 2 の装置とを有する情報共有システム。

【請求項 2 5】 複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用

いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第 1 の装置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第 2 の装置とを有する情報共有システム。

【請求項 2 6】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 2 4 または 2 5 記載の情報共有システム。

【請求項 2 7】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 2 4 または 2 5 記載の情報共有システム。

【請求項 2 8】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 2 4、2 5、2 6 または 2 7 記載の情報共有システム。

【請求項 2 9】 取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段を有する請求項 2 8 記載の情報共有システム。

【請求項 3 0】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とを少なくとも有する暗号化方法。

【請求項 3 1】 上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程をさらに有する請求項 3 0 記載の暗号化方法。

【請求項 3 2】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 3 0 または 3 1 記載の暗号化

方法。

【請求項 3 3】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 3 0 または 3 1 記載の暗号化方法。

【請求項 3 4】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 3 0、3 1、3 2 または 3 3 記載の暗号化方法。

【請求項 3 5】 複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する復号化方法。

【請求項 3 6】 複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、

選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する復号化方法。

【請求項 3 7】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項 3 5 または 3 7 記載の復号化方法。

【請求項 3 8】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項 3 5 または 3 6 記載の復号化方法。

【請求項 3 9】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項 3 5、3 6、3 7 または 3 8 記載の復号化方法。

【請求項 4 0】 取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する工程を有する請求項 3 9 記載の復号化方法。

【請求項 4 1】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特

定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、

上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えた情報処理方法。

【請求項42】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、

上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えた情報処理方法。

【請求項43】 上記付加情報は、暗号鍵のメッセージダイジェストである請求項41または42記載の情報処理方法。

【請求項44】 上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項41または42記載の情報処理方法。

【請求項45】 上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項41、42、43または44記載の情報処理方法。

【請求項46】 取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する工程を有する請求項45記載の情報処理方法。

【請求項47】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項48】 複数の暗号化鍵からユーザの秘密鍵で

暗号化鍵を復号し、暗号鍵を取得する工程と、

複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、

選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

10 【請求項49】 いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、

選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、

取得した暗号鍵に基づき暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項50】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、

上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項51】 情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、

上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコン

ピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、複数のユーザ間の情報共有を目的とし、情報の覗き見や改竄を防ぐための暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体に関するものである。

##### 【0002】

【従来の技術】近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報がコンピュータネットワーク上で利用されるようになった。しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

【0003】このような秘匿する必要がある情報を暗号化するために、データ暗号規格（DES ; Data Encryption Standard）などの共通鍵暗号方式が開発された。この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要がある。そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する手段が提案されている。

【0004】ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理する鍵管理システムや、情報を共有するユーザをグループ化して管理するグループ管理サーバ、情報へのアクセス制御手段などを利用する必要がある。

##### 【0005】

【発明が解決しようとする課題】ところで、共有したい秘匿情報毎に、情報を見てもよいユーザは異なる。しかしながら、たとえば、イントラネット上で、鍵管理システムやグループ管理サーバが構築されていたとしても、イントラネットにアクセス権限のない商談中の相手などと、秘匿情報を共有したい場合には、上述した手法では解決できない。

【0006】すなわち、上述した従来技術では、鍵管理システムや、グループ管理サーバ、アクセス制御手段などを利用しなければ、秘匿データを特定ユーザのみで、共有できないことから、インターネットなどの不特定多数のユーザがアクセスできるネットワーク上などでは、上記のようなシステムや手段を利用せずに、情報を共有できる環境を実現する必要がある。

【0007】本発明は、かかる事情に鑑みてなされたものであり、その目的は、鍵管理システムや、グループ管

理サーバ、アクセス制御手段などを利用しなくても、秘匿情報の複数ユーザによる共有が可能で、また、暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者に情報の内容を見られること防止できる暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体を提供することにある。

##### 【0008】

【課題を解決するための手段】上記目的を達成するため、本発明の暗号化装置は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段とを有する。

【0009】また、本発明の暗号化装置は、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段を有する。

【0010】また、本発明の暗号化装置は、上記複数の暗号化鍵および暗号化情報を転送する転送手段、または、上記複数の暗号化鍵、暗号化情報、および付加情報を転送する転送手段を有する。

【0011】また、本発明は、複数の暗号化鍵および暗号化情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【0012】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する暗号鍵取得手段と、上記付加情報に基づいて上記暗号鍵取得手段で取得された複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号化鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【0013】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基

10

20

30

40

50



づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【0014】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【0015】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【0016】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有

する暗号化装置と、上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【0017】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第1の装置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第2の装置とを有する。

【0018】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第1の装

置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第2の装置とを有する。

【0019】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第1の装置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第2の装置とを有する。

【0020】また、本発明の暗号化方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とを有する。

【0021】また、本発明の暗号化方法は、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程をさらに有する。

【0022】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する。

【0023】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザ

の秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する。

【0024】また、本発明の情報処理方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えている。

【0025】また、本発明の情報処理方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えている。

【0026】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とをコンピュータに実行させるプログラムが記録されている。

【0027】また、本発明の記録媒体は、複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な

暗号鍵を選択する工程と、選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムが記録されている。

【0028】また、本発明の記録媒体は、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムが記録されている。

【0029】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号化鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録されている。

【0030】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録されている。

【0031】本発明の暗号化系によれば、複数ユーザが共有したい情報を秘匿しておくために、たとえば共有鍵暗号方式と公開鍵暗号方式が併用される。入力情報は、共有鍵暗号方式で、暗号鍵を用いて暗号化される。次に、情報を共有する複数ユーザ各々の固有の公開鍵が、

取得もしくは、生成される。この複数の公開鍵各々で、暗号鍵が暗号化され、複数の暗号化鍵が生成される。これら暗号化鍵のうち一つは、あるユーザがこの情報を復号化するときに、そのユーザの秘密鍵を用いて復号化することによって、暗号鍵を作成することができる暗号化鍵である。これら複数の暗号化鍵と暗号化情報の両方が、複数ユーザで共有できる場所に転送される。

【0032】また、本発明に復号化系よれば、複数の暗号化鍵と暗号化情報を取得する手段を備えている。そして、取得した複数の暗号化鍵がユーザ固有の秘密鍵で復号化される。これにより得られた暗号鍵を利用して、暗号化情報が復号化されて、ユーザは、もとの情報を得ることができる。

【0033】さらに、本発明では、復号化時に取得した複数の暗号化鍵のうち、どの暗号化鍵がユーザの公開鍵で暗号化されたものかを特定するために、付加情報が添付される。この付加情報としては、暗号化系によって作成された、ユーザに関する情報や、暗号鍵に関する情報、暗号化鍵の順番に関する情報、もしくは、それらの情報を暗号化した情報や、それらの情報をもとにハッシュ関数などで作成されたメッセージダイジェストなどが利用される。また、付加情報は、複数の暗号化鍵や暗号化情報と共に複数ユーザで共有できる転送される。この付加情報を受け取った復号化系は、その内容をもとに、どの暗号化鍵をユーザの秘密鍵で復号化すれば、暗号鍵を得られるのかわかる。以上の2種の暗号化系および復号化系を利用することにより、複数のユーザのみで、情報を共有することができる。

【0034】また、本発明によれば、以上で説明した暗号化系と復号化系を利用した、ネットワーク上、または、単一装置（端末）上での情報共有システムが実現される。このシステムでは、上述したような暗号化系を組み込んだ端末を利用して、情報が暗号化される。ユーザは、情報を見てもよいユーザの公開鍵を特定することにより、共有するユーザを指定することができる。暗号化後、ネットワークを介して接続されているデータベースや、ファイルシステム、サーバーなどの情報保管装置に、暗号化情報、暗号化鍵、付加情報を転送し、保管される。また、上述した復号化系を組み込んだ装置を利用して、暗号化情報、暗号化鍵、付加情報が取得されて、暗号化情報が復号化されて、もとの情報を得ることができる。この情報の復号化時に、復号化しようとするユーザの公開鍵で暗号化された暗号化鍵がなければ、暗号鍵を生成できないので、第三者の覗き見、改竄を防ぐことができる。この情報共有システムでは、鍵管理システムやグループ管理サーバ、アクセス制御手段などを持たなくても、ユーザが利用する端末に、暗号化系や復号化系を組み込むだけで、情報を共有できるという利点がある。

【0035】また、現在、様々な共有鍵暗号方式、様々

な公開鍵暗号方式が提案されているが、本発明の暗号化系、復号化系では、様々な方式を利用することができる。そのため、様々な暗号方式の中でもどの方式を利用したのかを明確にする必要がある。本発明は、暗号化系で利用した暗号方式に関する情報（暗号方式情報）を、暗号化情報、暗号化鍵、付加情報と共に転送して、記憶装置に保管される。そして、復号化系では、暗号方式情報をもとに、復号化するための暗号方式が決定される。また、暗号化系と復号化系を組み込んだ一台以上の端末があれば、情報共有システムが実現できる。暗号化系を用いて上記の手順で情報を暗号化し、端末の記録装置に暗号化情報、暗号化鍵、付加情報を記録しておく。この端末を利用する別のユーザは、端末の記憶装置より暗号化情報、暗号化鍵、付加情報を取得し、復号化系を利用して、情報を得ることができる。この暗号化系、復号化系を利用すれば、鍵管理システムやグループ管理サーバ、アクセス制御手段を持たないパーソナルコンピュータなどでも、秘匿情報の複数ユーザによる共有が可能となる。

#### 【0036】

【発明の実施の形態】以下、本発明の実施形態を図面に関連付けて詳細に説明する。本実施形態では、本発明に係る暗号化装置および復号化装置のいずれか、または、両方が組み込まれた一台以上の端末と、暗号化情報、暗号化鍵、付加情報を格納するデータベース、もしくは、ファイルシステム、サーバがネットワークに接続された情報共有システム、および、本発明に係る暗号化装置および復号化装置にいずれか、または、両方が組み込まれた一台以上のネットワークに接続された端末で、そのうち一台以上の端末に暗号化情報、暗号化鍵、付加情報を格納できる機能が組み込まれている情報共有システムについて、順を追って説明する。

#### 【0037】第1実施形態

図1は本発明に係る情報共有システムの基本的な構成図、図2は本発明に係る暗号化装置の構成例を示すブロック図、図3は本発明に係る復号化装置の構成例を示すブロック図である。

【0038】本実施形態に係る情報共有システムは、図1に示すように、図2に示す暗号化装置10が組み込まれた第1の端末装置1、図3に示す復号化装置20が組み込まれた第2の端末装置2、並びに暗号化装置10で生成された複数の暗号化鍵、暗号化情報、および付加情報を保管するためのWWWサーバ3が、ネットワーク（たとえば、インターネット）4で接続されて構成されている。

【0039】第1の端末装置1に設けられた暗号化装置10は、暗号化部11、暗号鍵生成部12、記憶部13、暗号化鍵生成部14、付加情報生成部15、並びに転送部16により構成されている。

【0040】暗号化部11は、情報を暗号化するための

暗号鍵dkを用いて、たとえば共有鍵暗号方式（たとえばDES）により入力情報Mを暗号化して暗号化情報M'を生成し、生成した暗号化情報M'を転送部16に出力する。

【0041】暗号鍵生成部12は、たとえば乱数発生回路等により構成され、情報を暗号化するための暗号鍵dkを生成し、暗号化部11および暗号化鍵生成部14に出力する。なお、暗号鍵dkは、たとえば64ビットデータとして生成される。

【0042】なお、この暗号鍵dkを用いた情報の暗号化の一例のフローチャートを、図4に示す。

【0043】記憶部13は、たとえばハードディスクにより構成され、本システムを共有する複数nのユーザ各々の固有の公開鍵PK1, PK2, ..., PKnがあらかじめ記録されており、暗号化鍵生成部14によりアクセスされる。

【0044】暗号化鍵生成部14は、暗号化に用いた暗号鍵dkを、情報Mを記憶部13に記録されているユーザの公開鍵を用い、たとえば公開鍵暗号方式（たとえばRSA）に基づいて暗号化し、複数の暗号化鍵EK1, EK2, ..., EKnを生成し、生成した複数の暗号化鍵EK1, EK2, ..., EKnを転送部16に出力する。この暗号化鍵生成部14における、暗号鍵dkを公開鍵で暗号化し、複数の暗号化鍵を生成する動作のフローチャートを、図5に示す。

【0045】付加情報生成部15は、たとえば暗号鍵dkのメッセージダイジェストkmdをハッシュ関数などで生成し、付加情報ajfとして転送部16に出力する。なお、付加情報としては、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報であってもよい。この付加情報を生成する動作のフローチャートを、図6に示す。

【0046】転送部16は、入力情報Mの暗号化に伴って生成された複数の暗号化鍵EK1, EK2, ..., EK n、暗号化情報M'、および付加情報ajfをネットワーク4を介して保管手段装置としてのWWWサーバ3に転送する。

【0047】なお、暗号化装置10における上述した情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する、いわゆる暗号化処理工程を実行するためのプログラムは、第1の端末装置（コンピュータ）1で読み出し可

能な記録媒体、たとえば暗号化装置 10 やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第 1 の端末装置 1 で読み出されて実行される。

【0048】WWWサーバ 3 は、暗号化装置 10 から転送された入力情報 M の暗号化に伴って生成された複数の暗号化鍵 EK1, EK2, ..., EK<sub>n</sub>、暗号化情報 M'、および付加情報 a<sub>j</sub>f を受けて所定の記憶部に記録し、保管する。また、WWWサーバ 3 には、さらに、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報 desrsa (たとえば、DES と RSA で暗号化した、など) や、暗号化アルゴリズムの実行に必要な上記以外の情報 info (たとえば、DES に利用した初期化乱数など) も、一緒に保管されている。

【0049】第 2 の端末装置 2 に設けられた復号化装置 20 は、図 3 に示すように、暗号鍵取得手段としての暗号化鍵復号化部 21、暗号鍵選択部 22、および情報復号化部 23 により構成されている。

【0050】暗号化鍵復号化部 21 は、WWWサーバ 3 に保管されている複数の暗号化鍵を取得し、公開鍵暗号方式 (たとえば、RSA) を用いてユーザの秘密鍵 p<sub>v</sub>k で複数の暗号化鍵を復号して暗号鍵を取得し、暗号鍵選択部 22 に出力する。実際には、復号化された結果は、一つが所望の暗号鍵で残りは乱数である。なお、この複数の暗号化鍵の復号化動作のフローチャートを図 7 に示す。

【0051】暗号鍵選択部 22 は、WWWサーバ 3 に保管されている付加情報を取得し、この付加情報に基づいて、暗号化鍵復号化部 21 で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択して情報復号化部 23 に出力する。

【0052】この暗号鍵選択部 22 における暗号鍵の選択動作の具体例のフローチャートを図 8 に示す。暗号鍵選択部 22 は、図 8 に示すように、暗号化鍵復号化部 21 で取得された複数の暗号鍵を取得する (S221) とともに、WWWサーバ 3 に保管されている付加情報を取得する (S222)。そして、取得した付加情報より、複数の復号化された暗号化鍵の中に暗号鍵が含まれている否か判断する (S223, S224)。ステップ S224 において、複数の復号化された暗号化鍵の中に暗号鍵が含まれていると判断した場合には、復号化に利用する暗号鍵を決定し情報復号化部 23 に出力する (S225, S226)。一方、ステップ S224 において、複数の復号化された暗号化鍵の中に暗号鍵が含まれていないと判断した場合には、ユーザに復号化する権限がないものとして処理を中止する (S227)。

【0053】情報復号化部 23 は、WWWサーバ 3 に保管されている暗号化情報を取得し、暗号鍵選択部 22 で選択された暗号鍵に基づき暗号化情報を復号して元の情

報を取得する。この情報復号化部 23 の情報復号化動作のフローチャートを図 9 に示す。

【0054】なお、復号化装置 20 は、WWWサーバ 3 に複数の暗号化鍵、付加情報、および暗号化情報に加えて保管されている共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報 desrsa (たとえば、DES と RSA で暗号化した、など) や、暗号化アルゴリズムの実行に必要な上記以外の情報 info (たとえば、DES に利用した初期化乱数など) も、取得する。そして、たとえば、アルゴリズム識別情報 desrsa、情報 info に基づいて、復号化に利用できるように、アルゴリズムを初期化する。

【0055】また、復号化装置 20 における上述した上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する、いわゆる復号化処理工程とを実行するためのプログラムは、第 2 の端末装置 (コンピュータ) 2 で読み出し可能な記録媒体、たとえば復号化装置 20 やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第 2 の端末装置 2 で読み出されて実行される。

【0056】次に、上記構成による動作を説明する。なお、ここでは、第 1 の端末装置 1 を利用しているユーザ A は、他の 2 人のユーザ (B、C、) と計 3 人で、情報 M を共有したいと思っている場合を例に説明する。この場合、共有した秘匿情報 M を「こんにちは」、暗号鍵を 64 ビットのデータ「12345678」、ユーザ A の公開鍵を 512 ビットのデータ「Apublic...」、ユーザ B の公開鍵を 512 ビットのデータ「Bpublic...」、ユーザ C の公開鍵を 512 ビットのデータ「Cpublic...」、並びにユーザ C の秘密鍵を 512 ビットのデータ「Cprivate...」とする。

【0057】まず、第 1 の端末装置 1 の暗号化装置 10 では、記録媒体に記録されている暗号化プログラムが読み出されて、以下の処理が実行される。すなわち、入力情報 M (「こんにちは」) が暗号化装置 10 の暗号化部 11 に入力される。このとき、暗号鍵生成部 12 で、64 ビットデータである暗号鍵 dk (「12345678」) が生成され、この暗号鍵 dk が暗号化部 12 および暗号化鍵生成部 14 に供給される。

【0058】暗号化部 11 では、入力情報 M が共有鍵暗号方式 DES に基づいて暗号鍵 dk を用いて暗号化され、暗号化情報 M' (たとえば「#\$TA0x!h」) が生成されて転送部 16 に出力される。

【0059】ここで、暗号化装置 10 においては、暗号

化プログラムに基づいて、ユーザAに、誰と情報Mを共有したいのかを、尋ねられる。これに対して、ユーザAは、ユーザB、Cを図示しない入力部（たとえばキーボード）から入力する。この入力を受けて、暗号化装置10における暗号鍵生成部14によって、ユーザA、B、Cの公開鍵暗号方式（たとえば、RSA）に基づいた公開鍵PK1（「Apublic...」）、PK2（「Bpublic...」）、PK3（「Cpublic...」）が記憶部13から読み出される。そして、暗号鍵生成部14において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて暗号鍵dkが暗号化され、暗号化鍵EK1（「Adfjinme」）、EK2（「Zxcuqwez」）、EK3（「Pqueivnm」）が得られ、転送部16に出力される。

【0060】さらに、暗号化装置10の付加情報生成部15において、復号化時の暗号鍵dkを特定するための付加情報ajf（「' #Nv1am&」）、具体的には暗号鍵dkのメッセージダイジェストが作成され、転送部16に出力される。

【0061】そして、転送部16により、暗号化情報M'（「#\$TA0x!"h」）、暗号化鍵EK1（「Adfjinme」）、EK2（「Zxcuqwez」）、EK3（「Pqueivnm」）、付加情報ajf（「' #Nv1am&」）を含んだデータがネットワーク4を介してWWWサーバ3に転送され、たとえば図10に示すように所定の場所に保管される。また、WWWサーバ3には、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報desrsa（たとえば、DESとRSAで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報info（たとえば、DESに利用した初期化乱数など）も、一緒に保管されている。

【0062】次に、ユーザCが、Aの作成した情報Mを取得する場合を例に説明する。ユーザCは、まず、復号化装置20が組み込まれた第2の端末装置2を利用して、WWWサーバ3にアクセスし、暗号化情報M'（「#\$TA0x!"h」）、暗号化鍵EK1（「Adfjinme」）、EK2（「Zxcuqwez」）、EK3（「Pqueivnm」）、付加情報ajf（「' #Nv1am&」、メッセージダイジェストkmd）、アルゴリズム識別情報desrsa、情報infoを取得する。

【0063】復号化装置20では、まず、アルゴリズム識別情報desrsa、情報infoに基づいて、復号化に利用できるように、アルゴリズムが初期化される。そして、暗号化鍵復号化部21において、まず、暗号化鍵EK1（「Adfjinme」）、EK2（「Zxcuqwez」）、EK3（「Pqueivnm」）が、ユーザCの秘密鍵pvkC（「Cprivat

e...」）で、公開鍵暗号方式（たとえば、RSA）を用いて、復号化される。この場合、暗号化鍵EK1（「Adfjinme」）、EK2（「Zxcuqwez」）は、秘密鍵pvkC（「Cprivat e...」）で復号化しても、意味をもたない乱数rnA（たとえば乱数「00987232」）、rnB（たとえば乱数「50283740」）になるが、暗号化鍵EK3（「Pqueivnm」）は、暗号鍵dk（「12345678」）に変換される。

【0064】ここで、乱数2つと、暗号鍵dkが得られたが、実際には、3つとも、ビット列の形式をとるので、どれが、暗号鍵として用いることができるのか、分からない。そこで、復号化装置20の暗号鍵選択部22で、付加情報ajf（「' #Nv1am&」）を用いて、3つのビット列のうち、どれが、暗号鍵なのかを選択されて、暗号鍵が特定される。この場合には、乱数rnA、rnB、暗号鍵dkのメッセージダイジェストが付加情報として生成されており（たとえば、MD5などを利用して）、それらのうち、WWWサーバ3より取得したメッセージダイジェストkmdと一致するメッセージダイジェストが生成したビット列（この場合は、dk）が、暗号鍵として、選択される。

【0065】本例の場合、乱数「00987232」、乱数「50283740」、暗号鍵「12345678」のメッセージダイジェストが作成され、それぞれmes1「hine@han」、mes2「uineb'&v」、mes3「' #Nv1am&」である場合には、mes3が付加情報として等しいことから、3つ目の「12345678」が暗号鍵として特定できる。

【0066】そして、情報復号化部23において、選択された暗号鍵dk（「12345678」）を利用することによって、暗号化情報M'（「#\$TA0x!"h」）が共有鍵暗号方式（たとえば、DES）を用いて復号化されて、もとの情報M（「こんにちは」）が得られる。

【0067】以上説明したように、本第1の実施形態によれば、複数のユーザでアクセス可能なWWWサーバ3と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化部11と、暗号化に用いた暗号鍵を、情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成部14と、生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成部15と、複数の暗号化鍵、暗号化情報、および付加情報をWWWサーバ3に転送し保管させる転送部16とを有する暗号化装置10を備えた第1の端末装置1と、保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号化鍵復号化部21と、保管されている付加情報を取得して当該付加情報に



に基づき取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択部22と、選択された暗号鍵に基づき保管されている暗号化情報を復号して元の情報を取得する情報復号化部23とを有する復号化装置20を備えた第2の端末装置2とを設け、これらをネットワーク4で接続したので、情報の復号化時に、復号しようとするユーザの公開鍵で暗号化された暗号化鍵がなければ、暗号鍵を生成できないので、第三者の覗き見、改竄を防ぐことができる。この情報共有システムでは、鍵管理システムやグループ管理サーバ、アクセス制御手段などを持たなくても、ユーザが利用する端末に、暗号化系や復号化系を組み込むだけで、情報を共有できるという利点がある。

#### 【0068】第2実施形態

本第2の実施形態では、暗号化装置10が組み込まれた第1の端末装置1、復号化装置20が組み込まれた第2の端末装置2が、ネットワーク（たとえば、LAN）で接続されている場合の例を、以下に説明する。

【0069】この場合は、WWWサーバは不要であり、その代わりに第1の端末装置1の記憶装置が用いられる。また、第2の端末装置2の復号化装置20aは、たとえば図11に示すように、第1の端末装置1の記憶装置に保管されている付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択部24と、暗号化鍵選択部で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得部25と、暗号鍵取得部25で取得された暗号鍵に基づき取得した複数の暗号化鍵および付加情報とともに保管されている暗号化情報を復号して元の情報を取得する情報復号化部26とを有するように構成される。なお、図3に示す復号化装置が本第2の実施形態に適用できることはいうまでもない。

【0070】次に、本第2の実施形態の動作について説明する。ここでは、第1の端末装置1を利用しているユーザAは、他の3人のユーザ（B、C、D）と計4人で、情報Mを共有しているものとする。ユーザAは、暗号化装置10を利用して、情報Mを暗号化して、第1の端末装置1の情報保管機能（たとえば、ハードディスクのファイルシステム）に暗号化情報を保管しておく。

【0071】まず、第1の端末装置1の暗号化装置10では、記録媒体に記録されている暗号化プログラムが読み出されて、以下の処理が実行される。すなわち、入力情報Mが暗号化装置10の暗号化部11に入力される。このとき、暗号鍵生成部12で、暗号鍵dkが生成され、この暗号鍵dkが暗号化部12および暗号鍵生成部14に供給される。

【0072】暗号化部11では、入力情報Mが共有鍵暗号方式DESに基づいて暗号鍵dkを用いて暗号化され、暗号化情報M'が生成されて転送部16に出力される。

【0073】ここで、暗号化装置10においては、暗号化プログラムに基づいて、ユーザAに、誰と情報Mを共有したいのかを、尋ねられる。これに対して、ユーザAは、ユーザB、C、Dを図示しない入力部（たとえばキーボード）から入力する。この入力をうけて、暗号化装置10における暗号鍵生成部14によって、ユーザB、C、Dの公開鍵暗号方式（たとえば、RSA）に基づいた公開鍵PKB、PKC、PKDが記憶部13から読み出される。そして、暗号鍵生成部14において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて暗号鍵dkが暗号化され、暗号化鍵EKB、EKC、EKDが得られ、転送部16に出力される。

【0074】さらに、暗号化装置10の付加情報生成部15において、たとえば、暗号化鍵EKB、EKC、EKDとユーザB、C、のID、idB、idC、idDを対応づける対応表mtBCDが付加情報として作成される。これらの情報を生成終了すると、転送部16により暗号化情報M'、暗号化鍵EKB、EKC、EKD、対応表mtBCDが第1の端末装置1の記憶装置（たとえば、ハードディスク）に保管される。また、第1の端末装置1の記憶装置には、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報desrsa（たとえば、DESとRSAで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報info（たとえば、DESに利用した初期化乱数など）も、一緒に保管されている。

【0075】次に、ユーザCが、Aの作成した情報Mを取得する場合を例に説明する。ユーザCは、まず、復号化装置20が組み込まれた第2の端末装置2を利用して、第1の端末装置1の記憶装置をアクセスし、暗号化情報M'、暗号化鍵EKB、EKC、EKD、付加情報ajf（対応表mtBCD）、アルゴリズム識別情報desrsa、情報infoを取得する。

【0076】復号化装置20では、まず、アルゴリズム識別情報desrsa、情報infoに基づいて、復号化に利用できるように、アルゴリズムが初期化される。ここでは、暗号化鍵EKB、EKC、EKDの3つの暗号化鍵が得られたが、実際には、3つとも、ビット列の形式をとるので、どれを復号化して、暗号鍵として用いることができるのか、分からない。そこで、暗号鍵選択部24で、付加情報（この場合は、対応表mtBCD）を用いて、3つのビット列のうち、どれが、暗号鍵なのかが選択される。そして、対応表より、暗号化鍵復号部25において暗号化鍵EKCがユーザCの秘密鍵pvkCで、公開鍵暗号方式（たとえば、RSA）を用いて、復号化され、暗号鍵dkが得られる。

【0077】そして、情報復号化部26において、復号化暗号鍵dkを利用することによって、暗号化情報M'が共有鍵暗号方式（たとえば、DES）を用いて復号化

されて、もとの情報Mが得られる。

【0078】以上説明したように、本第2の実施形態においても、上述した第1の実施形態の効果と同様の効果を得ることができる。

【0079】なお、上述した第1および第2の実施形態では、第1の端末装置1には暗号化装置10のみを設け、第2の端末装置2には暗号化装置20のみを設けた場合を例に説明したが、これに限定されるものではなく、第1および第2の端末装置1、2に暗号化装置10および復号化装置20の両方を組み込むことも可能であり、この場合も上述したと同様の効果を得ることができる。

【0080】この場合、端末装置1、2においては、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録媒体、第1および第2の端末装置1、2やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第1および第2の端末装置1で読み出されて実行される。

【0081】このように両方の端末装置1、2に、復号化系を組み込んでおくと、端末1を利用するユーザDも、端末装置1を使って、上記の方法で、情報Mを得ることができる。また、このように暗号化、復号化の両系を一つの端末に組み込んでおけば、端末装置1だけで、情報共有システムが実現できる利点がある。

【0082】また、上述した第1および第2の実施形態では、暗号化処理工程および復号化処理工程を実行するためのプログラムが記録され、コンピュータで読み出し可能な記録媒体として、暗号化装置、復号化装置やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等を例に説明したが、

これに限定されるものではなく、他の例として、たとえばインターネットの専用線や電話回線等の通信線路のように、通信プログラムを伝送する際にこの通信プログラムを一定時間保持するデータ伝送路等を挙げることができる。

#### 【0083】

【発明の効果】以上説明したように、本発明によれば、鍵管理システムや、グループ管理サーバー、アクセス制御手段などを利用しなくても、秘匿情報の複数ユーザによる共有が、可能となる。また、暗号化情報を保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

#### 【図面の簡単な説明】

【図1】本発明に係る情報共有システムの基本的な構成図である。

【図2】本発明に係る暗号化装置の構成例を示すブロック図である。

【図3】本発明に係る復号化装置の構成例を示すブロック図である。

【図4】暗号鍵を用いた情報の暗号化の一例を示すフローチャートである。

【図5】暗号化鍵生成部における、暗号鍵を公開鍵で暗号化し、複数の暗号化鍵を生成する動作を示すフローチャートである。

【図6】付加情報を生成する動作のフローチャートである。

【図7】複数の暗号化鍵の復号化動作を示すフローチャートである。

【図8】暗号鍵選択部における暗号鍵の選択動作の具体例を示すフローチャートである。

【図9】情報復号化部の情報復号化動作を示すフローチャートである。

【図10】WWWサーバに記録されるデータ例を示す図である。

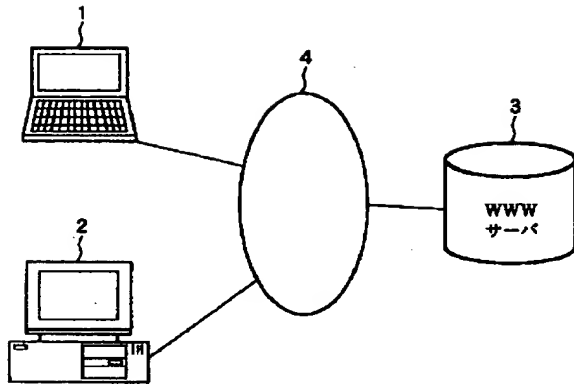
【図11】本発明に係る復号化装置の他の構成例を示すブロック図である。

#### 【符号の説明】

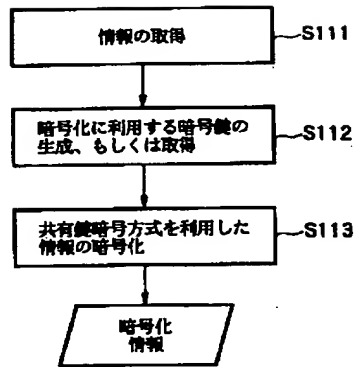
1…第1の端末装置、2…第2の端末装置、3…WWWサーバ（情報保管装置）、4…ネットワーク、10…暗号化装置、11…暗号化部、12…暗号鍵生成部、13…記憶部、14…暗号化鍵生成部、15…付加情報生成部、16…転送部16、20…復号化装置、21、25…暗号化鍵復号化部、22…暗号鍵選択部、23、26…情報復号化部、24…暗号化鍵選択部。



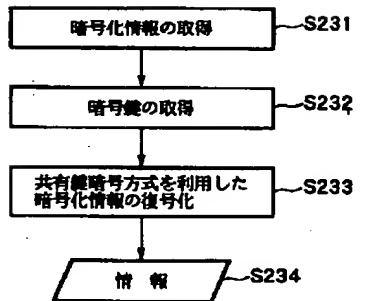
【図 1】



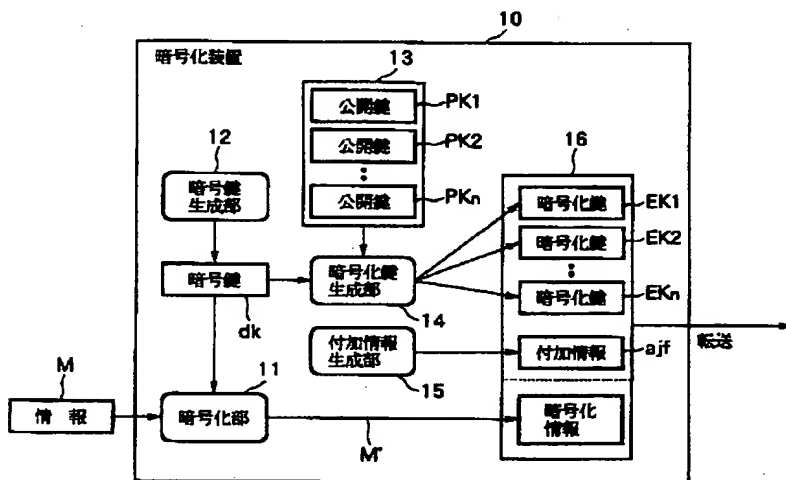
【図 4】



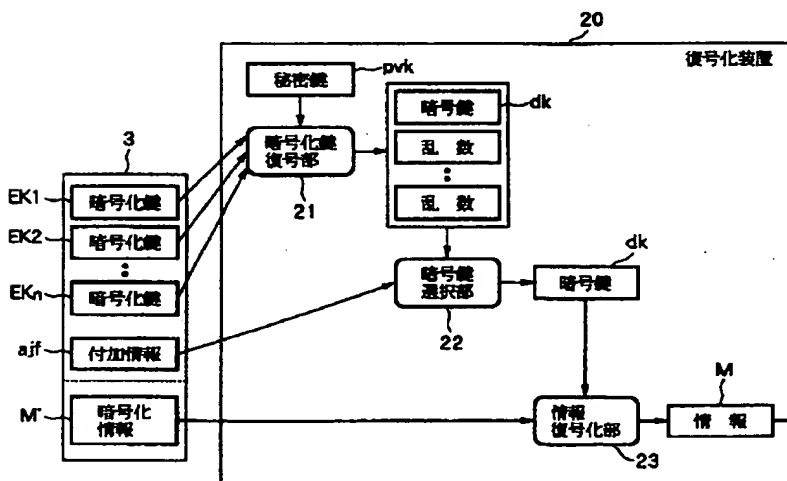
【図 9】



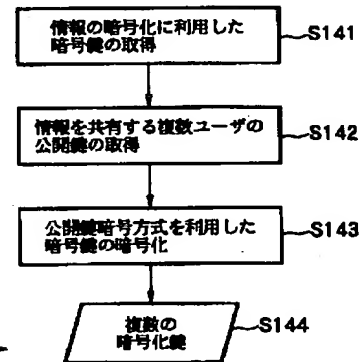
【図 2】



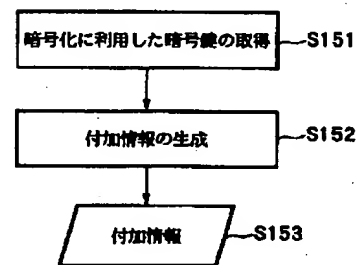
【図 3】



【図 5】



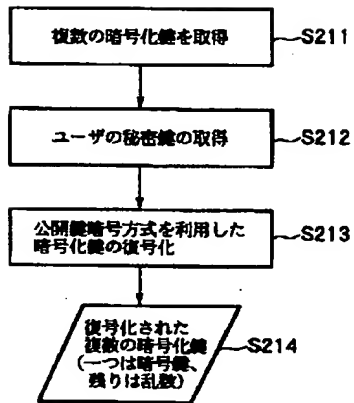
【図 6】



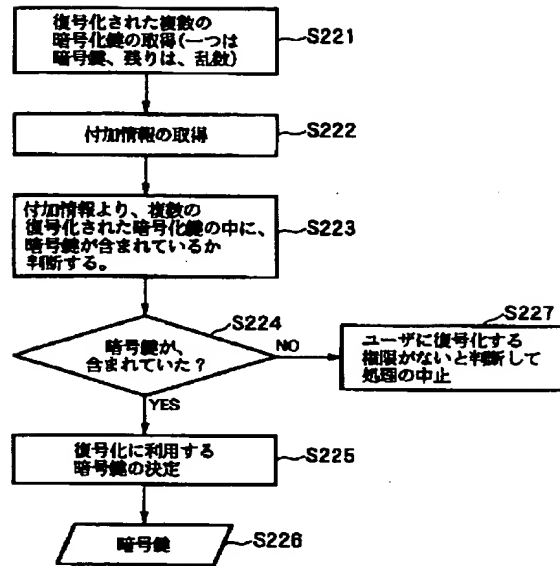
【図 10】

Key	Adffinme
Key	Zacuqwez
Key	Pqneivnm
Info	' # Nviam &
Content	# \$ TA0x1 "h

【図 7】



【図 8】



【図 11】

